UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,072	02/26/2004	Yohsuke Ishii	MEI-101	3877

24956 7590 09/20/2007

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
DARNO, PATRICK A	

ART UNIT	PAPER NUMBER
2163	

MAIL DATE	DELIVERY MODE
09/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,072	ISHII ET AL.	
	Examiner	Art Unit	
	Patrick A. Darno	2163	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. No new claims have been added. Claims 1-16 and claims 18-28 remain cancelled. Claim 17 has been amended. Claim 17 is pending in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2004/0254934 issued to Mang-Rong Ho et al. (hereinafter "Ho") in view of U.S. Patent Application Publication Number 2005/0091658 issued to Jude Jacob Kavalam et al. (hereinafter "Kavalam") in view of U.S. Patent Number 5,260,551 issued to Tore Wiik et al. (hereinafter "Wiik") in view of U.S. Patent Application Publication Number 2004/0203589 issued to Jiwei R. Wang et al. (hereinafter "Wang") and further in view of U.S. Patent Application Publication Number 2004/0153552 issued to Dirk Trossen et al. (hereinafter "Trossen").

Claim 17:

The combination of Ho, Kavalam, Wiik, Wang, and Trossen discloses an access control system in which a plurality of storage devices for storing information resources and access controllers for controlling accesses to the information resources stored in the storage devices are connected with a network, each of the access controllers having an access control list on which access right to each information resources stored in the storage devices is recorded, and each of

the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices,

and Ho discloses each access controller comprising:

an access restriction module *(Ho: paragraph [0004], lines 1-9 and paragraph [0009], lines 7-9 and paragraph [0010], lines 7-9; The content management system is the access restriction module.)* configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller that records access right to each information resource *(Ho: paragraph [0003], lines 2-9 and paragraphs [0028]-[0031] and paragraph [0078], lines 6-10; Note specifically in the first reference cited "storage of an access control list (ACL) for each data entity to which access is to be controlled." Paragraph [0001], lines 9-11 defines a data entity.).*

Ho does not explicitly disclose:

an access interception module configured to restrict the access by reference to the access prohibition list of the access controller, which records user information of access prohibited users, prior to the access control list;

an access control list update module configured to update the access control list according to the access prohibition list;

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or updated access prohibition list to the other access controllers in response to the update; and

the other access controllers further comprising a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list thereof to include the received user information or updated access prohibition list,

wherein the distribution module of each access controller sends out the user information or the updated prohibition list to a predetermined other one of the access controllers, thereby transmitting the user information or the updated prohibition list from one access controller to another, and

wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

Kavalam also discloses an access control module to control access to network resources with the use of access control lists *(Kavalam: Fig. 1, 116 and paragraph [0062], lines 5-8)*. Examiner notes that Kavalam does not explicitly disclose the use of an access prohibition list (or black-list) to intercept or restrict user access, but Kavalam does explicitly suggest protecting system resources by strategies such as "lock down", isolation, and sandboxing of users or systems when either accidental or malicious actions occur that could harm system resources *(Kavalam: paragraph [23], lines 23-28)*. In order to "lock down", isolate, or sandbox a particular user or system, a system administrator would have to have some means to detect that an accidental or malicious act which either has already occurred, is currently occurring, or may occur in the future.

In order to satisfy the suggestion of combining additional methods of protecting system resources with the use of an access control module using access control lists, examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ho, as suggested by Kavalam with the teachings of Wiik noted

below *(Note that Kavalam is not being used as prior art for any particular claim limitation. Kavalam is cited for the sole purpose of providing a suggestion to combine Ho and Wiik.).*

Wiik explicitly discloses:

an access interception module configured to restrict the access by reference to the access prohibition list of the access controller, which records user information of access prohibited users *(Wiik: column 5, lines 7-9; The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to add the user's name to the black-list. This immediately cancels the user's action rights and effectively 'intercepts' the access of the user.)*;

an access control list update module configured to update the access control list according to the access prohibition list *(Wiik: column 4, lines 31-38 and column 5, lines 7-11; The access control list of each lock is updated based on upon the black list (access prohibition list).)*;

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or updated access prohibition list to the other access controllers in response to the update *(Wiik: column 5, 7-11 and column 5, lines 56-63 and column 4, lines 32-38; The "lock communicator" (or admin access controller) oversees each individual locking mechanism (or access interception module or access controller). Since the lock communicator controls the access controller (locking mechanism), the lock communicator itself is also an access controller. From the cited references it can be see that the lock communicator (access controller) downloads (updates) new user information (user ID) to the black-list. The transfer of this information from the lock communicator to the locking mechanism must be done through a distribution module. Note specifically that the*

claim language recites 'AT LEAST ONE...' The Examiner has interpreted the claim such that only one access controller comprises a distribution module.); and

the other access controllers further comprising a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list thereof to include the received user information or updated access prohibition list *(Wiik: column 5, lines 9-11; The black-list is updated by the lock communicator (or admin access controller) according to user ID's. Note that the update to the black list is received at the access controller (locking mechanism). There must be some form of receiving module to receive the update. Further note that the update to the black-list can be an addition ("lock communicator is used to fill the list with black listed ID's") or deletions ("lock communicator also has an un-black-list function").).*

wherein the distribution module of each access controller sends out the user information or the updated prohibition list to a predetermined other one of the access controllers, thereby transmitting the user information or the updated prohibition list from one access controller to another *(Wiik: column 4, lines 35-38 and column 5, lines 7-11; Note the lock communicator (admin access controller) sends out newly added user ID's to the black-list (prohibited list) which is stored in the RAM of individual access controllers (locking mechanisms). This updates the black-list. Further note that lock communicator (admin access controller) is used to configure all locking mechanisms (access controllers) (Wiik: column 5, lines 56-59). Since it is assumed that only one access controller has a distribution module (see Examiner's comments above), this limitation is not given patentable weight because it refers to something that essentially can't occur. Since only one access controller has a distribution module, additional access controllers cannot keep transferring the prohibition lists. Due to this interpretation, the cited combination of references still discloses all limitations of the Applicant's claimed invention.).*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a black-list, or prohibited user list, as part of an access controller *(Wiik: column 5, lines 7-11)*. The skilled artisan would have been motivated to improve the invention of Ho per the above such that upon making a decision to cancel a given individual's access rights, the individual could be added to a black-list resulting in the immediate loss of access to a given resource *(Wiik: column 5, lines 7-11 and column 8, lines 11-14)*.

The previously mentioned combination of Ho, Kavalam, and Wiik does not explicitly disclose restricting access by first referencing a prohibited list **prior to** the access control list.

However, Wang discloses restricting access by first referencing a prohibited list **prior to** the access control list *(Wang: paragraph [0033] lines 1-3; The black-list is the prohibited list and the while-list is the access allowed list.)*.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the previously mentioned combination with the teachings of Wang noted above for the purpose of modifying the order in which the lists are accessed. The skilled artisan would have been motivated to further improve the previously mentioned combination per the above such that the system is capable of checking a black list of access rights prior to checking an access rights allowed list *(Wang: paragraph [0033], lines 1-3)*. Checking the smaller black list first can result in saving processing time because the system may not have to search the larger white list.

The previously mentioned combination of Ho, Kavalam, Wii, and Wang does not explicitly disclose wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

However, it should be noted for the record though that Wiik does explicitly suggest providing access rights for only a certain predetermined period of time *(Wiik: column 2, lines 17-20 and column 3, lines 19-20; In the first reference note specifically "card validity time". And in the second reference note specifically the "start work time" and the "stop work time". These times represent times when the access to a certain access controller will start and stop respectively.).*

Furthermore, Trossen discloses wherein the list update module deletes the user information on the access prohibition list at a predetermined timing *(Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; In order to clarify the record, all that the applicant is claiming here is simply the changing of access rights at a predetermined period of time. By deleting the user information from the prohibition list, the access rights of the user are no longer blocked. The user may have access again to all resources if added to appropriate access control lists, but that much is not stated here. The references cited from the Trossen reference clearly show a changing of access rights at a certain predetermined period of time. Further, in the second reference cited above, Trossen shows deleting this the users information from the database when the subscription ends. When the subscription ends, the user no longer has access to the resources granted by the subscription. This subscription ends at a predetermined period of time. The examiner maintains that the Trossen reference and invention claimed by the applicant are performing exactly the same function, and therefore the two inventions are not patentably distinct, because they both perform the same operation, in essentially the same manner, of canceling access rights at a predetermined period of time.).*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Trossen noted above for the purpose of including an expiration time for access rights *(Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14).* The skilled artisan would have been motivated to improve the previously mentioned combination per the above such that upon reaching a certain

predetermined time, a status change notification message could be displayed showing the change in access rights of a user *(Trossen: paragraph [0002], lines 14-17; The examiner would like to bring to the applicant's attention that the reason or motivation to modify the reference may often suggest what the inventor has done, but for a different purpose or to solve a different problem. It is not necessary that the prior art suggest the combination to achieve the same advantage or result discovered by the applicant (In re Linter, 173 USPQ 560 (CCPA 1972) and In re Dillon, 16 USPQ2d 1897 (Fed. Cir. 1990)).).*

Response to Arguments

Examiner Notes:

The Applicant's arguments with respect to the Ho, Kavalam, Wiik, and Wang references appear to have already been presented by the Applicant in previous correspondence with the Examiner. The Examiner's stance on these matters has not changed. The Applicant is directed to the Examiner's Office Actions mailed 05/03/2006, 10/23/2006, and 04/05/2007 in order to refresh the Applicant on the Examiner's position.

The newly added claim limitations have failed to place the claim 17 in condition for allowance. Therefore, claim 17 remains rejected under 35 U.S.C. 103(a) as unpatentable in view of the combination of references cited in the preceding office action.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrick A. Darno whose telephone number is (571) 272-0788. The examiner can normally be reached on Monday - Friday, 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Don Wong can be reached on (571) 272-1834. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DON WONG
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Patrick A. Darno